Data Privacy in a Time of Covid-19: *How concerned are you?*

R. Trestian | Middlesex University, UK
G. Xie | Dublin City University, Ireland
P. Lohar | Dublin City University, Ireland
E. Celeste | Dublin City University, Ireland
M. Bendechache | Dublin City University, Ireland
R. Brennan | Dublin City University, Ireland
E. Jayasekera | National College of Ireland, Ireland
R. Connolly | Dublin City University, Ireland
I. Tal | Dublin City University, Ireland

***Abstract*—We introduce a study examining people's privacy concerns in a time of Covid-19 and we reflect on people's willingness to share their personal data in the interest of controlling the spread of the virus and save lives.**

The significant growth in the number of users with mobile phones as well as the adoption of key enabling technologies like cloud computing has led to the creation of an entire tracking ecosystem that could enable the use of pervasive surveillance methods. However, this development also brings serious privacy concerns, as current governance and regulation frameworks are lagging behind these technological advancements. This is visible in the current pandemic, where concerns around privacy and civil liberties have led several countries to respond differently in their approach of controlling the spread of Covid-19 and preserve human life.

This article aims to answer the following questions: (1) What is the general attitude towards privacy in a time of Covid-19? (2) Has this attitude changed compared to normal circumstances with the desire to help control the spread of Covid-19? (3) Do privacy concerns prevent people from using technologies (e.g. COVID Tracker app) that may help in managing the crisis? (4) Are people concerned about the long term influence of these technologies (beyond the health crisis) on their privacy? To answer our questions, we conducted a case study in the Republic of Ireland and a questionnaire was distributed online at a national level. The survey was created using Google Forms. Data collected is covered by the Dublin City University Google Apps agreement which includes data protection assurances. The survey has been approved by the National Research Ethics Committee of the Health Research Board in Ireland. We report here the results of this national survey that collected 1001 effective responses from 1012 participants.

Our main finding is that there is a significant shift in the attitude of the Irish population towards privacy during the pandemic.

Privacy and Health Data

Although no-one has examined whether privacy attitudes towards personal health data change during a pandemic, a time when the trade-off between risks and benefits is dramatically accentuated, the literature does provide guidance as to the nature of data privacy concerns and how they can motivate behavior. For example, attention has been paid to understanding how data privacy concerns influence technology adoption behaviors in relation to a number of health artifacts, ranging from examinations of electronic health record adoption to wearable healthcare devices. A consistent motif throughout this literature is that privacy dilemmas in relation to health information are unique, as the risk associated with its disclosure are distinctive both in nature and variety. For example, the disclosure decision is characterized by a high level of risk and uncertainty regarding collection, secondary usage, errors, improper access, control and awareness of personal health information [2]. As a consequence, theoretical stances employed in the information privacy literature [3] tend towards a cognitive and consequentialist emphasis where individuals weigh up the costs and benefits associated with a behavior. Much reliance has been placed on expectancy theory which proposes that the individual is motivated to choose a particular action based on their evaluation of the desirability of positive outcomes resulting from that behavior. Decisions then result from engaging in this cognitive assessment of how likely the expected results of a behavior will result in the desired positive outcome, known as a valence. In a data privacy context, this assessment is known as the privacy calculus and it proposes that the intention to disclose is influenced by the balancing of potential privacy concerns with information disclosure benefits. Although this model has been widely used [4], it contains limitations as the evaluation of expected risks and benefits associated with information disclosure have been shown to differ according to context and it also neglects the relationship between information privacy concerns and their antecedents. In this study, we identify the factors influencing data privacy concerns in relation to a tracking app specific to the context of a pandemic.

Data Privacy in Contact-Tracing Apps

In the current Covid-19 global pandemic environment, a proliferation of contact-tracing applications has been developed, the success of which relies on obtaining access to citizen's mobile phone GPS location and other personal data. While some countries have adopted a forced mass surveillance method that limits individual freedoms, other countries with a strong democratic and civil liberty ethos are encouraging voluntary adoption of contact-tracing applications by their citizens. This requires that a large proportion of the population consent to sharing location and other personal data in order to improve tracking and suppress spread of the virus. As a result, the pandemic is testing attitudes towards privacy and government surveillance.

Consequently, in an attempt to overcome security and privacy concerns, various Covid-19 tracing apps have adopted different architectures for data collection. These architectures are predominantly classified into two categories [5], [6]: (1) centralized, and (2) decentralized. The classification is determined by the way in which the server is used and the type and location of the data collected as seen in **Figure** 1.

Within the *centralized architecture* most of the information is stored and processed on a centralized cloud server. In this approach, the cloud server plays a key role by storing pseudonymous users' personal information, performing risk analysis and sending out notifications to close contacts in case of infection. Consequently, this raises security and privacy concerns regarding the use and the life cycle of the data collected especially should the cloud server become an untrustable entity. However, the information stored on the centralized server can be employed for data analysis that could help the government when making decisions regarding lockdown restrictions in hot-spot areas.

In a *decentralized architecture*, the core functions are moved to user devices, which results in involvement of the centralised server within the contact tracing process being drastically reduced. This approach tries to enhance user privacy by

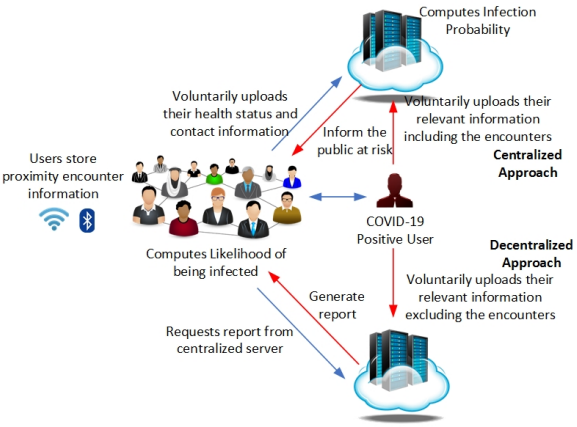

Figure 1. Centralized vs. Decentralized Approach of Contact Tracing Apps

performing the tracing process locally on the user's device. Contact tracing apps that are based on the decentralized approach do not require the users to pre-register prior to use and as consequence, no personal identifiable information is stored on the server. Any device running the app will generate privacy-preserving pseudonyms that are exchanged periodically between the devices that come in close contact. The central cloud server in this scenario acts as a rendezvous point for lookup purposes where the infected user can volunteer to upload their relevant time information which reflects only their individual trajectory and does not include any information about the encounters. Other app users can regularly access this type of information from the central server, using it locally on their devices for risk analysis purposes, to check if they have been exposed to the virus and for how long. Even though this approach alleviates some of the privacy risks, no information is stored on the central server for data analysis purposes that could help the government when making decisions regarding lockdown restrictions in exposed hot-spot areas.

Overview of Contact Tracing Apps

In terms of the technology being used, both the centralized and decentralized approaches predominantly rely on Bluetooth, Global Positioning System (GPS), Quick Response (QR) codes and cellular location tracking [7]. A summary of the contact tracing apps adopted by different countries around the world, including their names and their corresponding technologies is illustrated in **Figure** 2.

However, regardless of the technology being used, the main technical requirements of any contact tracing app is that it must operate at close range in order to be able to determine with high accuracy if a person has been within the 2m proximity of an infected individual. While GPS is capable of providing accurate location information between 10 to 20 meters only, cellular location data is even less precise and contributes to significant privacy concerns regarding the violation of citizens' data protection rights. Consequently, most contact tracing apps rely on Bluetooth which operates at close range and has a reasonable accuracy within the 2m proximity. More importantly, the individual remains in control and can decide whether to opt in or out by switching the Bluetooth function on or off. As seen in **Figure** 2, most countries rely on Bluetooth as the best choice regardless of the approach implemented.

Countries like France, Australia, Singapore, New Zealand, Norway, India, Mexico, Qatar, Kuwait, Bahrain, Hungary, Bulgaria, Tunisia have opted for centralized approaches. The centralized apps mainly follow the PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) protocol [8]. Most of the centralized approaches combined Bluetooth with location information to improve the accuracy. However, in Norway the Data Protection Authority has suspended the app on the grounds that poses a significant threat to user privacy by continuously uploading individuals' location information. In the UK a centralized approach was initially adopted, but due to privacy concerns and mobile devices battery drainage, a switch was made to decentralized solution. Belgium, Switzerland, Finland, Estonia adopted the decentralized approach that follows the DP-3T (Decentralized Privacy-Preserving Proximity Tracing) [9] which is seen as a partially decentralized solution as it uses an anonymous centralized database for the infected individual. However, the identification of a specific individual is not possible through the type of data collected and exchanged. Recently, most of the countries adopted the decentralized approach that relies on the cross-platform API developed by Google and Apple [10]. However, despite the

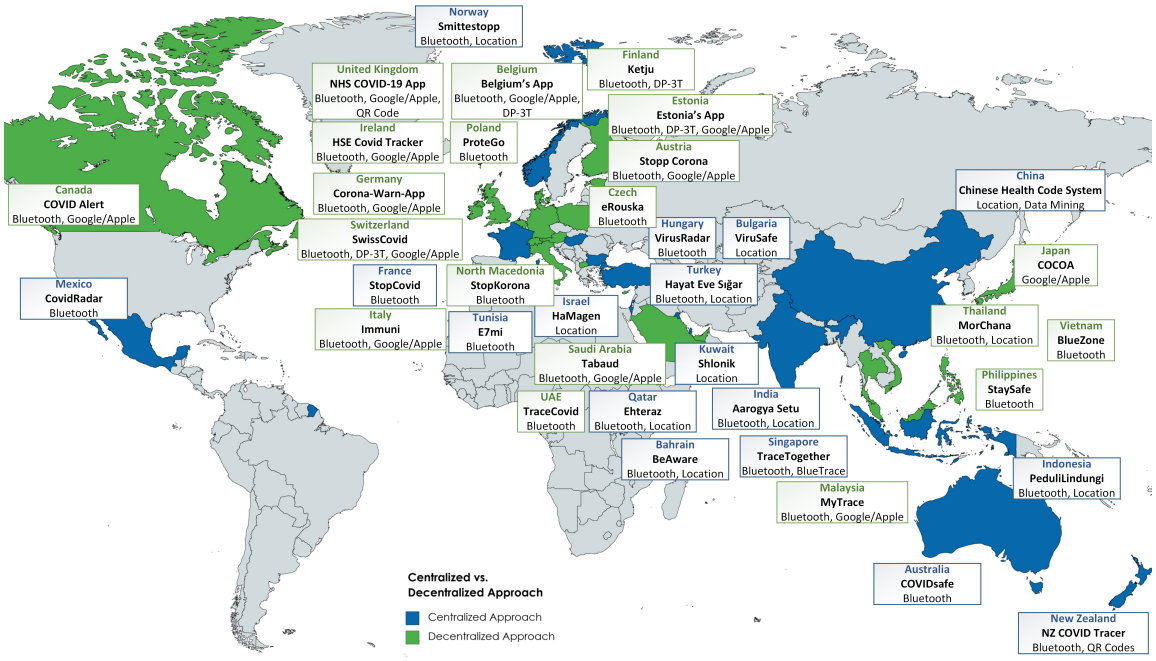

Figure 2. Centralized vs. Decentralized Contact-Tracing App Approaches Around the World and Technologies Involved

improvements around privacy and security, there are still concerns that Google/Apple could end up controlling the EU's Covid-19 app ecosystem. For example, in Ireland Health Service Executive (HSE) addressed the privacy issues of their Covid Tracker app by making the assessment on data protection impact of the app available to the public, and the source code of the app was also made open source. However, the Irish Council for Civil Liberties raised privacy concerns due to the lack of transparency from Apple and Google's side in terms of their involvement in the tracker app.

Despite all the efforts across the world, it is obvious that finding the balance between the potential benefits of an effective technology-based contact tracing app and the data protection and privacy of individuals remains a challenge.

Attitudes to Privacy in a Time of COVID-19

Since privacy concerns drive the technical requirements for many tracing apps, it is vital to understand the public's views on privacy. Consequently, we conducted a study to investigate the attitudes to privacy of the residents of Ireland during Covid-19 times. The study is based on an anonymous questionnaire that was distributed online over the main channels at national level during 12th Nov. 2020 and 12th Jan. 2021. The questionnaire is structured in three parts: (1) demographic data collection following the guidelines from [11]; (2) set of questions to model the general privacy profiles based on the Privacy Segmentation Index (PSI) [12]; and (3) questions that aim to capture the attitude towards privacy in times of Covid-19.

Of all 1001 participants, 489 (48.85%) are male and 490 (48.95%) are female, 18 people choose preferring not to say and 4 people choose Non binary. The largest age group is between 25-44 years old with 503 participants which account 50.0% of total. Regarding the participants' location, most of the participants (62.3%) come from county Dublin. The remaining 37.7% of the participants are distributed among the rest of the counties. The participants are well-educated, with 30.3% owning a Master's degree, 22.2% a Bachelor's degree and 16.8% finished secondary school. The participants sample seems to be a good representation of the Irish population and in line with the 2016 Census data [13]. However, it is worth acknowledging that the participants' characteristics within the sample might limit the

generalization of the results.

General Privacy Profiles

To identify the general privacy profile of each participant, we introduced three statements in the second part of the questionnaire, as follows:

1) *Consumers have lost all control over how personal information is collected and used by companies;*
2) *Most businesses handle the personal information they collect about consumers in a proper and confidential way;*
3) *Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.*

The participants could rate them between *Strongly Disagree* to *Strongly Agree* on a four-point scale. Based on their response to these statements, we classified the participants into three groups: (a) *privacy fundamentalists*, representing individuals that are at the maximum extreme of the privacy concern and the most protective of their privacy; (b) *privacy pragmatists*, a grouping that represents those individuals who weigh up the pros and cons of information sharing before making a decision to share their personal information; and finally (c) the *privacy unconcerned*, a group representing those individuals who are least protective of their privacy. In line with Westin's classification [12] participants who agreed with statement 1 and disagreed with statements 2 and 3 were profiled as *privacy fundamentalists*. Participants who disagreed with statement 1 but agreed with statements 2 and 3 were profiled as *privacy unconcerned*, while the rest of the participants were profiled as *privacy pragmatists*.

The results of the general privacy profiles of the participants in our national questionnaire indicate that 29% of participants were *privacy fundamentalists*, 54% were *privacy pragmatists* and 17% were *privacy unconcerned*. These results are consistent with the results of previous Westin's surveys which indicated that the majority of the participants were privacy pragmatists [12].

Privacy Attitudes in a Time of Covid-19

To understand if there is any shift in attitude in terms of data privacy in times of Covid-19 as compared to normal circumstances, the answers to two questions from the third part of the questionnaire were analysed. The two questions relate to the participants' willingness to share their personal data (data stored on their mobile device) with the government and relevant institutions/organizations under normal circumstances vs. their willingness to do so during this specific time of pandemic. The results are illustrated in **Figure** 3 and are grouped according to Westin's classification. Additionally, in order to understand if the shift in attitude is statistically significant, a paired t-test was conducted where $p - value = 1.0666E - 138$. This gives a strong evidence that the change in attitude towards data sharing during pandemic as compared with normal circumstances is statistically significant.

We notice that there is a shift in attitude, with 61% of the participants indicating that they Strongly Agree and Agree to share their mobile data during Covid-19 as compared to 14% before the pandemic. 55% of the participants changed their attitude from Strongly Disagree, Disagree or Neutral to Agree and Strongly Agree. Considering the sample size of 1001 participants from a 4.9 million population of Ireland we can state with a confidence interval of 95% that between 52% and 58% of the entire relevant population would shift their attitude towards sharing their mobile data during a pandemic in the interest of saving lives. In terms of *privacy fundamentalists* around 31% (a combined response of Strongly Agree and Agree) of them would change their attitude towards mobile data sharing in times of Covid-19. Previous studies [14] have indicated that the more aware of privacy threats people become the higher their feeling of concern, which makes it more likely for them to be profiled as *privacy fundamentalists*, even though their actions in general might not justify their classification. Most noticeably and, perhaps, not surprisingly, the highest shift in attitude is recorded by the *privacy unconcerned* with a jump of 57%, followed by privacy fundamentalists and privacy pragmatists with an increase of 46% and 44%, respectively.

To better understand the privacy attitude shift, we asked the participants to indicate what type of mobile data would they agree to share and with what organizations or sectors will they be willing to share this data in order to help defeat the Covid-19 outbreak. The participants could

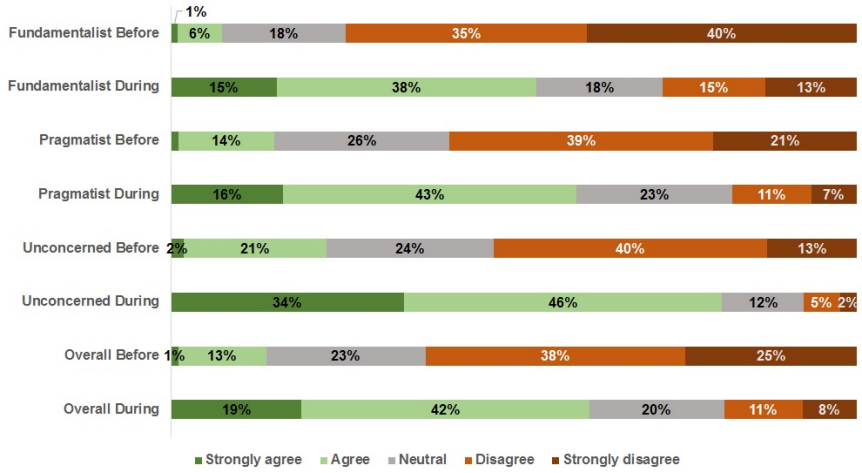

Figure 3. Willingness to share the personal data before and during Covid-19

choose multiple answers for these questions, consequently the highest number of selections was recorded by *anonymized mobile geo-location data (not exact location, but within a range)* followed by *Health status data* as listed in **Table 1**. **Table 2** highlights the top organizations or sectors that the participants would be willing to share their mobile data with. We notice that out of the institutions listed, people trust most the HSE and least the private players involved.

Using the COVID Tracker app

Of all the participants 79% indicated that they are familiar with the HSE COVID Tracker app and its role, while 12% are neutral and the rest of 9% are not familiar. However, only 62% of the participants indicated that they are using the COVID Tracker app, with 60% of them finding the app helpful in controlling the virus. We use the Pearson's chi-square test to understand if there is any association between being familiar with the app and actually using the app. The test results revealed a p-value of $1.11521E-56$ indicating that there is sufficient evidence to conclude that there is a relationship between the two statements. Consequently, the participants that are familiar with the HSE COVID Tracker app and its role tend to actually use the app as well. Moreover, regardless of the participants attitude shift during pandemic, 60% of the participants Strongly Agree and Agree with the statement that *Digital tracking technologies are important to help control Covid-19 spread and monitor public health"*. Even from those who are not using the COVID Tracker app, 35% still agree or strongly agree with this statement. This indicates that people believe that digital tracking technologies are useful and could help control the pandemic.

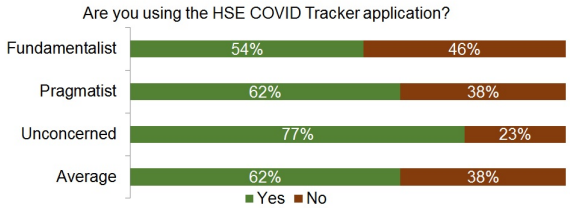

Figure 4. HSE COVID-19 Tracker App adoption per privacy group

Figure 4 shows the adoption of the application by the three different privacy groups. The privacy fundamentalist people are the group with the lowest adoption of the application. This suggests that privacy concerns seem to prevent the adoption of tracking technology, even in a global pandemic situation.

Concerns on Privacy

In order to understand people's concerns on privacy we requested the participants to indicate their concern level on a five-point scale from *Not concerned at all* to *Extremely Concerned* when asked: *Would you be concerned in relation to how your personal data would be used by the government and the relevant institutions in order*

Table 1. Types of mobile data to be willingly shared by participants

What type of mobile data would you agree to share?	Count
Anonymized mobile geo-location data (not exact location, but within a range)	653
Health status data	619
Personal details (name, gender, age)	411
Exact mobile geo-location data	321
Contact list	206
Other	84

Table 2. Organizations or Sectors participants would agree to share their mobile data with

With which of the following would you be willing to share your mobile data?	Count
Public Health authorities like HSE	859
Government	482
Public apps sharing anonymized data	366
Private/commercial apps sharing anonymized data	147
Private Health Companies/Agencies	105
Public apps sharing individual data	57
Private/commercial apps sharing individual data	18
Other	54

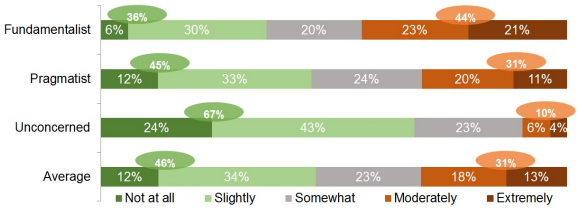

Figure 5. Concern levels on how the personal data might be used

to defeat Covid-19?

Our results (**Figure 5**) indicate that overall 46% of the participants are *Not concerned at all* and *Slightly Concerned*. However, the fundamentalists who are the most privacy concerned group of people prove to be the ones with the lowest adoption rate of the app among all the participants. Hence the attitude towards privacy is an influencing factor in the adoption of the app. However, looking into the specific concerns of the participants we ranked them as follows: (1) privacy issues; (2) lack of trust in the Government and the institutions managing the data; (3) security issues; (4) creating a dangerous precedent; (5) other. Moreover, only 15% of the participants would be *Extremely concerned* if their mobile data would be transferred to other countries within the EU in order to defeat Covid-19.

The participants that are using or have used the HSE COVID Tracker app, were also asked to indicate their concern about what happens/happened to their information (for example how long it is retained for) once they quit using the application or once the pandemic is over. The results indicate that 42% of the respondents are concerned about what happens with their information once they quit using the COVID-19 Tracker app. Moreover, approximately 30% of the respondents stated that they *worried that the application will be used as a tool of surveillance beyond the scope of COVID-19*. While 28% stated that they are *worried about the implications this application will have on [my] privacy and data protection*.

Survey Feedback Analysis

All the participants were asked to leave their comments/feedback on the survey. Out of 1012 participants, we received 202 comments with most of them being about the COVID tracker application. To better understand the comments, we manually inspected and divided them into three classes depending upon the degree of underlying sentiment: (i) *negative*: if the comment expresses dissatisfaction, unhappiness, complaint etc.; (ii) *neutral*: if the comment is a query, information etc regardless of any sentiment; and (iii) *positive*: if the comment expresses satisfaction, happiness etc. We observed that more than half (50.71%) of the comments express negative opinions on the COVID Tracker application. In contrast, only 13.57% are positive comments about the COVID Tracker app in terms of data privacy considerations, with one respondent commenting *"I went through the data policy on the tracker app and am confident using it in terms of my data privacy." [respondent comment]* while another respondent said *"The COVID 19 tracker has been*

well designed with respect to privacy considerations. It is a good model for how such apps should be developed."[respondent comment] The rest 35.71% of the comments are neutral, i.e, either they are simply providing information or are queries, regardless of any sentiment.

The feedback from the participants in the survey unveiled another theme relevant to the tracking apps in general and COVID Tracker app in particular: their efficacy. The participants expressed doubts about the efficacy of the tracker app with several respondents commenting:

"I use the covid tracker but note that I hear little about how useful it is thought to have been - Silence after the initial hype" [respondent comment]

"I uninstalled the COVID Tracker app as it did not work when my housemates got COVID, and it was taking up a lot of storage in my phone." [respondent comment]

People are also unhappy about the lack of communication of conclusive data showing the efficacy of the app with one respondent commenting:

"Use of tracker system to date in Ireland UK(?): Real impact / success = ?" [respondent comment]

The survey results show, that in order to reinforce the trust in the contact tracing apps and to stimulate their adoption, the transparent communication of success stories of the apps and data showing their efficacy is extremely important.

Formal Legality vs. Legal Reality

As seen in Figure 4, 62% of the respondents confirmed their use of the COVID Tracker app. However, only 52% of the participants using the app confirmed that they have read the privacy policy. Interestingly, 30% feared that the app could be used as a surveillance tool going beyond its primary aim to fight the spread of Covid-19 and another 28% stated that they had privacy concerns regarding the app.

We argue that these data show a discrepancy between formal legality and legal reality, or, in other words, between what is formally legal and what is perceived as such. Moreover, privacy concerns related to the potential misuse of mobile apps introduced to fight Covid-19 are not unfounded. For example, in some countries, contact tracing apps process location data and have been used by government for general law enforcement purposes, a circumstance that the European Data Protection Board in its Guidelines published in April 2020 has defined as *"a grave intrusion into people's privacy"* [15]. Similar risks have generated an intense debate in Europe on the safeguards that contact tracing apps should guarantee in line with EU fundamental rights. To this end, last spring, the European Commission, the European Data Protection Board and the European eHealth Network adopted detailed sets of guidance on how to deploy digital technology solutions in full respect of EU fundamental rights.

In Ireland, the Department of Health and the HSE successfully demonstrated to comply with these guidelines in developing and introducing the COVID Tracker App. Therefore, notwithstanding the formal legality of the digital solutions implemented in Ireland, the results of the survey show a significant mistrust in the safeguards the Irish app is theoretically meant to guarantee. In conclusion, this image of legal reality in Ireland indicates the need to reflect on the capability of existing data protection law to be understood and instill trust at societal level.

Conclusions

The integration of contact-tracing apps in emergency responses could represent a dramatic shift when dealing with public health interventions, such as the current spread of Covid-19. However, privacy and legal concerns around data sharing hinder the adoption and consequently the efficacy of these contact-tracing apps. We have conducted a study on the privacy attitude in a time of Covid-19, of the people living in Ireland. Our results showed that people in Ireland are aware and protective of their privacy, but there is a change in their attitude during the pandemic. In general, people showed an increased willingness to share their personal data (including location, contacts, and medical data) in the interest of saving lives from 14% pre-pandemic to 61% during pandemic.

Our study shows that enhancing transparency and data protection literacy is of utmost importance. Adequate information should be provided to data subjects in order to express their consent, even if other legal bases for data processing are

available. Due to a mistrust of tech companies by the population, a greater reliance on public institutions is recommended. Involvement of the wider population in early phases of decision-making processes related to the employment of digital technology solutions to fight Covid-19 is crucial to enhance the level of legitimacy of the adopted solutions and as a trigger of greater transparency of the decision-making processes. Where public-private partnerships are employed, all choices affecting data protection and privacy of individuals should be made in a transparent manner and highlighted in order to minimise the discrepancy between formal legality and legal reality.

ACKNOWLEDGMENT

This work was supported by Science Foundation Ireland through COVID Rapid Response programme grant number 20/COV/0229 and through the grant 13/RC/2094 co-funded under the European Regional Development Fund through the Southern and Eastern Regional Operational Programme to Lero - the Irish Software Research Centre (www.lero.ie) and the ADAPT Centre for Digital Content Technology (www.adaptcentre.ie) [grant number 13/RC/2106]

REFERENCES

1. D. Skoll, J. C. Miller, L. A. Saxon, ”COVID-19 testing and infection surveillance: Is a combined digital contact-tracing and mass-testing solution feasible in the United States?,” in *Elsevier Cardiovascular Digital Health Journal*, Oct. 2020.
2. W. Hong and J. Y. L. Thong, ”Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies”, MIS Quarterly, vol. 37, no. 1, 2013, pp. 275–298.
3. T. Dinev and P. Hart, ‘An Extended Privacy Calculus Model for E-Commerce Transactions’, Information Systems Research, vol. 17, no. 1, Mar. 2006, pp. 61–80.
4. H. Xu, H.-H. Teo, B. Tan, and R. Agarwal, ‘The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services’, J. Manage. Inf. Syst., vol. 26, no. 3, Dec. 2009, pp. 135–174.
5. M. A. Azad et al., ”A First Look at Privacy Analysis of COVID-19 Contact Tracing Mobile Applications”, arXiv:2006.13354 [cs], Aug. 2020, Accessed: Oct. 21, 2020. [Online]. Available: http://arxiv.org/abs/2006.13354.
6. D. Wang and F. Liu, ”Privacy Risk and Preservation For COVID-19 Contact Tracing Apps”, arXiv:2006.15433 [cs], Jun. 2020, Accessed: Oct. 21, 2020. [Online]. Available: http://arxiv.org/abs/2006.15433.
7. J. Li and X. Guo, ”COVID-19 Contact-tracing Apps: a Survey on the Global Deployment and Challenges”, arXiv:2005.03599 [cs], May 2020, Accessed: Oct. 21, 2020. [Online]. Available: http://arxiv.org/abs/2005.03599.
8. PEPP-PT Consortium, ”Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT),” *White Paper*, June, 2020. Accessed: Nov. 30, 2020. [Online] Available: https://github.com/pepp-pt/pepp-pt-documentation;
9. C. Troncoso et. al., ”Decentralized Privacy-Preserving Proximity Tracing,” *White Paper*, May, 2020. Accessed: Nov. 30, 2020. [Online] Available: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf;
10. Apple and Google, ”Exposure Notification API launches to support public health agencies,” *Press Release*, May, 2020. Accessed: Nov. 30, 2020. [Online]. Available: https://blog.google/inside-google/company-announcements/apple-google-exposure-notification-api-launches/;
11. J. Hughes et al. “Rethinking and Updating Demographic Questions: Guidance to Improve Descriptions of Research Samples.” *Psi Chi Journal of Psychological Research*, vol. 21, 2016, pp. 138-151.
12. P. Kumaraguru and L. F. Cranor, ”Privacy Indexes: A Survey of Westin’s Studies”, (CMU-ISRI-5-138) *Technical report*, Institute for Software Research International, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 2005.
13. Central Statistics Office, ”Census of Population 2016 – Profile 10 Education, Skills and the Irish Language”, *Census of Population 2016*, Ireland, April, 2016. Accessed: Jun. 6, 2021. [Online] Available: https://www.cso.ie/en/census/
14. J. Tsai, L. F. Cranor, A. Acquisti, and C. M. Fong, ”What’s it to You? A Survey of Online Privacy Concerns and Risks”, *Social Science Research Network*, Rochester, NY, SSRN Scholarly Paper ID 941708, Oct. 2006.
15. European Data Protection Board, ”Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak,” April, 2020. Accessed: Dec. 09, 2020. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_en;

R. Trestian is a Senior Lecturer with Middlesex Univ., London, UK. She received her Ph.D. degree from Dublin City Univ. in 2012. Her research interests include mobile and wireless communications, machine learning, user perceived quality of experience, multimedia streaming, handover and network selection strategies. She is an Associate Editor of the IEEE Commun. Surveys & Tutorials. Contact email: r.trestian@mdx.ac.uk.

G. Xie is a Research Assistant at Dublin City University. His research interests are in the field of natural language processing, especially machine translation. Recently, his work is focused on low-resource language and constraint decoding methods of machine translation. Contact email: guodong.xie@adaptcentre.ie.

P. Lohar is a Research Assistant at Dublin City University. He obtained his PhD degree from Dublin City University in 2020. His research interests are Machine Translation and Natural Language Processing. Contact email: pintu.lohar@adaptcentre.ie.

E. Celeste is an Assistant Professor in Law, Technology and Innovation with Dublin City University. His research interests include digital rights and constitutionalism, privacy and data protection law, online platforms governance and regulation. He is the principal investigator of 'Digital Constitutionalism: In Search of a Content Governance Standard' funded by Facebook Research, and 'Cross-Border Data Protection' funded by the Irish Research Council and the UK Economic and Social Research Council. Contact email: edoardo.celeste@dcu.ie.

M. Bendechache is an Assistant Professor with Dublin City University, Ireland. She obtained her Ph.D. degree from University College Dublin, Ireland in 2018. Her research interests include Big Data Analytics, Machine Learning, Data Governance, Cloud Computing, Blockchain, Security and Privacy. She is an academic member of ADAPT and LERO research centres. Contact email: malika.bendechache@dcu.ie.

R. Brennan is an Assistant Professor with Dublin City University, Chair of the DCU MA in Data Protection and Privacy Law and a Funded investigator in the Science Foundation Ireland ADAPT Centre for Digital Content Technology which is funded under the SFI Research Centres Programme (Grant 13/RC/2106) and is co-funded under the European Regional Development Fund. His main research interests are data protection, data value, data quality, data privacy, data/AI governance and semantics. Contact email: rob.brennan@dcu.ie.

E. Jayasekera is a Lecturer in Computing with National College of Ireland. She received a Specialist degree in Information Security in 2008 from Kursk State Technical University, Russia and was also awarded a Ph.D from the St. Petersburg National Research University of Information Technologies, Mechanics and Optics in 2013. She specializes in data privacy and security and holds an international patent in data anonymization. Contact email: evgeniia.jayasekera@ncirl.ie.

R. Connolly is a Professor of Information Systems with Dublin City University. She is a co-founder of the Centre for eIntegrated Care at DCU. Her work has been published in prestigious international journals and her research focuses on inclusion and successful adoption of Information Technology, within public sector transformation contexts, with particular emphasis on digital information privacy. She is a lead partner in research projects that have received over €21 million in EU Horizon funding and is also a Funded Investigator with LERO, the Irish Software Research Centre. Contact email: Regina.Connolly@dcu.ie.

I. Tal is an Assistant Professor with School of Computing, Dublin City University in Ireland, Academic Lead of the MSc in Blockchain and member of LERO. She received her Ph.D. degree from the School of Electronic Engineering, Dublin City University, Ireland. Her research interests include technology enhanced learning, vehicular ad-hoc networks, smart cities and cyber security. She is the Lead Principal Investigator on the SFI funded project PRIVATT. She published in prestigious international conferences and journals. Contact email: irina.tal@dcu.ie.